Department of Veterans Affairs
Washington DC, 20420

VA HANDBOOK 6502.4
Transmittal Sheet
November 16, 2009

PRIVACY ACT REVIEWS

1. REASON FOR ISSUE: This Handbook clarifies Department-wide procedures for Privacy Act reviews.

2. SUMMARY OF CONTENTS AND /MAJOR CHANGES: This Handbook updates Department-wide procedures for Privacy Act reviews that were previously contained in VA Handbook 6300.5. The responsible office has also changed.

3. RESPONSIBLE OFFICE: Assistant Secretary, Office of Information and Technology (005), Deputy Assistant Secretary, Information Protection and Risk Management (005R), Office of the Associate Deputy Assistant Secretary for Privacy and Records Management (005R1), and the VA Privacy Service (005R1A) is responsible for the material contained in this Handbook.

4. RELATED DIRECTIVE AND HANDBOOKS: VA Directive 6502, VA Enterprise Privacy Program; VA Directive 6300, Records and Information Management: and VA Handbooks 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act; 6300.5, Procedures for Establishing and Managing Privacy Act System of Records, 6309, Collection of Information Procedures, and 6300.7, Procedures for Computer Matching Programs.

5. RESCISSIONS: None.

CERTIFIED BY:

/s/

Roger W. Baker
Assistant Secretary for Information
and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/

Roger W. Baker
Assistant Secretary for Information
and Technology

Distribution: Electronic Only

PRIVACY ACT REVIEWS

CONTENTS

PARAGRAPH **PAGE**

PRIVACY ACT REVIEWS

1. PURPOSE. This Handbook sets forth procedures for conducting reviews as required by the Privacy Act of 1974 (5 U.S.C. 552a). The Department of Veterans Affairs (VA) must conduct regularly scheduled reviews of the implementation and administration of certain provisions of the Privacy Act as outlined in Appendix I of Office of Management and Budget (OMB) Circular A-130. While formal biennial Privacy Act reports are no longer required, VA must be prepared to report to the Director of OMB on the results of these reviews. In addition, VA provides a summary of the Department's compliance with these reviews as part of its annual reporting requirements under the Federal Information Security Management Act of 2002 (FISMA) (Title III, Pub. L. No. 107-347) and Agency Privacy Management Report.

2. RESPONSIBILITIES OF THE SYSTEM MANAGER. The Privacy Act requires that each agency designate an agency official who is responsible for each System of Records. This person is known as the System Manager. The System Manager is usually the Information Owner, as defined by VA Handbook 6500, Information Security Program, an official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. The System Manager is responsible for:

a. Ensuring the policies, practices, and procedures governing the maintenance of records in a system are being followed;

b. Working with the Information System Owner and the Information Security Officer (ISO) to ensure appropriate management, operational, physical, administrative, and technical safeguards are in place to prevent unauthorized disclosure or alteration of information in the system, including a review of whether records are downloaded to a personal computer or removable storage devices (such as thumb drives, external hard drives, compact discs (CDs), digital versatile discs (DVDs) and cell phones) to be managed, stored or manipulated. Downloads such as these may lead to the creation of new, unauthorized systems of records;

c. Confirming records contain only such information about an individual that is relevant and necessary to accomplish a purpose of the agency to be accomplished by statute or by Executive Order of the President;

d. Ensuring the information in the system is accurate, timely, complete, relevant and necessary to accomplish a VA mission;

e. Maintaining an accounting of disclosures;

f. Guaranteeing routine uses are compatible with the purposes for which the information was collected;

g. Working with the Privacy Officer or designee to ensure procedures for access, correction, or amendment of records conform to the requirements of this Handbook, VA Handbook 6300.4, and VHA Handbook 1605.1, and that VA regulations governing the Privacy Act are followed;

h. Reviewing each system of records notice (SORN) annually to ensure it accurately describes the system of records;

i. Reviewing each routine use statement every three years to ensure the disclosures of records under each routine use are still compatible with the purpose for which the information was collected;

j. Ensuring the description of recordkeeping practices in the retention and disposal portion of the SORN reflects the retention and disposal of the records schedule approved by the Archivist of the United States; and in the event there is no approved retention and disposal period for the records, initiating immediate action to obtain the approval of the Archivist of the United States;

k. Determining whether the system of records may be exempted from certain provisions of the Privacy Act (5 U.S.C. 552a(j) and (k)), taking the necessary steps to invoke the exemptions, and if the system of records is exempt, reviewing the exemption every three years to determine if the exemption is still needed; and

l. Conducting detailed risk assessments of new or altered systems of records to ensure appropriate administrative, technical, and physical safeguards are established to protect records in the system from unauthorized disclosure, alteration or access.

3. DESCRIPTION OF PRIVACY ACT REVIEWS. VA must conduct regularly scheduled reviews of the implementation and administration of certain provisions of the Privacy Act as outlined in Appendix I of OMB Circular A-130. While formal biennial Privacy Act reports are no longer required, VA must be prepared to report to the Director of OMB on the results of these reviews. OMB provides detailed guidance each year on what information needs to be included in the annual FISMA reports and Privacy Management Report. Appendix A, Schedule of Privacy Act Reviews, identifies each review item, the action office(s), the frequency of review, and the action required. The following is a brief description of these review activities.

a. **Section (m) Contracts**. If a contractor maintains a system of records on behalf of VA to accomplish an agency function, then all of the provisions of the Privacy Act apply to that system of records, and the provisions of 5 U.S.C. 552a(m) are binding on the contractor and its employees. Every two years, a sample of these contracts is reviewed to ensure the wording of each contract includes these provisions. ***Note***: the Federal Acquisition Regulation provides two clauses – 52.224-1, Privacy Act Notification, and 52.224-2, Privacy Act – that are to be added to these contracts.

b. **Recordkeeping Practices**. VA's department recordkeeping and disposal policies and practices are reviewed annually to assure compliance with the Privacy Act. Particular attention should be given to automated systems of records.

c. **Routine Use Disclosures**. All routine use disclosures associated with each system of records subject to the Privacy Act are reviewed every three years to ensure that each use of the records continues to be compatible with the purpose for which the Department collected the information (5 U.S.C. 552a(a)(7) and (b)(3)).

d. **Exemption of Systems of Records**. Each system of records for which VA has promulgated exemption rules pursuant to Section (j) or (k) of the Privacy Act is reviewed every three years to determine whether such exemption is still needed.

e. **Computer Matching Programs**. Each ongoing computer matching program in which the Department has participated during the year, either as a source or recipient agency, is reviewed to ensure the requirements of the Privacy Act, the OMB matching guidance, and VA Handbook 6300.7, Procedures for Computer Matching Programs, have been met.

f. **Systems of Records Notices (SORN)**. Each SORN is reviewed annually to ensure it accurately describes the system, and it contains current administrative information, such as titles of VA officials, addresses, or office symbols (5 U.S.C. 552a(e)).

g. **Privacy Act Training.** Training procedures are reviewed to ensure all VA employees are familiar with the requirements of the Privacy Act, VA's implementing regulations, and any special requirements of their specific jobs. ***Note***: VA Directive 6502, VA Enterprise Privacy Program, provides more details on the design, development, delivery, and monitoring of privacy training for VA employees.

h. **Violations.** VA employees are required to report any potential privacy violations or breaches to their ISO and Privacy Officer, and these are processed pursuant to VA Handbook 6500.2, Management of Security and Privacy Incidents. In addition, pursuant to the Privacy Act, the Department will review annually, the circumstances and actions of VA employees that resulted in VA being found civilly liable under Section (g) of the Privacy Act, or an employee being found criminally liable under the provisions of Section (i) of the Privacy Act. The purpose of this review is to determine the problem and find the most effective way to prevent recurrence.

i. **Section (e)(3) Statements.** VA informs each person whom it asks to supply information on why their information is being collected and how it will be used. A Privacy Act statement appears on the form which is used to collect the information or on a separate form that can be retained by the person (see VA Directive 6309, Collection of Information Procedures, for further information). The Privacy Act statement will include the following:

(1) Authority to collect the information and whether the disclosure of such information is mandatory or voluntary;

(2) Principal purpose or purposes for which the information is intended to be used;

(3) Routine uses that may be made of the information; and

(4) The effects on the person, if any, of not providing all or any part of the requested information.

4. DEFINITIONS

a. **Disclosure.** Providing information from a system of records, by any means, to anyone other than the individual by whose name or other identifier the record is retrieved.

b. **Individual.** A living citizen of the United States or an alien lawfully admitted for permanent residence. ***Note***: The definition of "individual" for Privacy Act purposes differs from the definition of "individual" for Freedom of Information Act (FOIA) purpose. Deceased persons, non-resident aliens, businesses, and organizations are not individuals under the Privacy Act.

c. **Information System Owner**. As defined by VA Handbook 6500, the Information System Owner is an official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

d. **Maintenance.** To collect, keep, use, disseminate, or any combination of these recordkeeping functions. As used in the Privacy Act, VA regulations, and this Handbook, these words mean control over and, therefore, responsibility and accountability for systems of records.

e. **Record.** Any item, collection, or grouping of information about an individual that is maintained by the Department, such as, but not limited to, the individual's education, financial transactions, personal history, or medical history, and that contains the individual's name or identifying number, symbol, or other identifying characteristic assigned to the individual, such as a fingerprint, voice print, or a photograph. The definition does not distinguish between data and information. Both are within the scope of the definition.

f. **Routine Use**. This term is unique to the Privacy Act and means the disclosure of a record for a reason that is compatible with the purpose for which it was collected. A routine use is one that is relatable and necessary to a purpose for collecting the record. To be effective, a routine use must be properly published in the *Federal Register*.

g. **System Manager**. The official responsible for the management, operation, and release of information from a system of records subject to the Privacy Act. The System Manager is usually the Information Owner. As defined by VA Handbook 6500, this is an official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

h. **System of Records**. Any group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying characteristic assigned to the individual. A record in a system of records must contain two elements: a personal identifier and at least one item of personal information. If a retrieval of personal information is possible, but not actually done, or if it depends on memory or a sequential search, the collection of records is not a system of records. However, creating a retrieval method or cross-index arranged by personal identifier for randomly filed records makes that record collection a system subject to the provisions of the Privacy Act.

SCHEDULE OF PRIVACY ACT REVIEWS

Review Item	Action Office(s)	Frequency of Review	Action Required
1. Section (m) Contracts	Office of Acquisitions and Logistics	Every two years	1. Develop a plan to accomplish review. 2. Perform review.
2. Recordkeeping Practices	Each VA Central Office organizational element	Annually	1. Develop plan and procedures to accomplish review. 2. Ensure that procedures cover field locations. 3. Perform review.
3. Routine Use Disclosures	Each VA Central Office organizational element that manages or operates a system of records subject to the Privacy Act	Every three years	1. Develop and plan procedures to accomplish review. 2. Identify each system of records for which routine use changes or deletions must be made, the specific routine use statement to be changed or deleted, and the reason for the change or deletion. 3. Prepare *Federal Register* notice and related paperwork.
4. Exemptions of System of Records	Each VA Central Office organizational element that manages an exempt system of records	Every three years	1. Review each exempt system of records.
5. Computer Matching Programs	Each VA Central Office organizational element that manages systems of records used for a new, existing, or renewed computer matching program	Annually	1. Perform review (results are also reported in VA's Biennial Computer Matching Activities Report).
6. System of Records Notice (SORN)	Each VA Central Office organizational element that manages a system of records	Annually	1. Review each SORN for which it is responsible. 2. Identify any system of records that needs to be changed and describe what the changes are. 3. Prepare *Federal Register* notice and related paperwork.

7. Privacy Act Training	VA Privacy Service	Annually	1. Design, develop, and deliver annual privacy training. 2. Monitor training for VA employees, contractors, volunteers, interns and trainees. 3. Work with other VA Central Office organizational elements to develop appropriate role-based training as necessary.
8. Violations	Office of Risk Management and Incident Response	Annually	1. Obtain reports of any violations. 2. Review reports and, as necessary, work with other VA Central Office organizational elements to develop or change procedures to prevent a reoccurrence. 3. Civil or criminal violations are referred to the Office of the Inspector General and Office of General Counsel.
9. Privacy Act Statements	Each VA Central Office organizational element that manages a system of records	Every three years	1. Follow the procedures outlined in VA Handbook 6310.2, Information Collection of Procedures.